NLdigital

Version: July 2024

Data Processing Agreement Boltrics Professionals BV

Comprised of:
Deel 1. Data Pro statement
Deel 2. Standard Clauses for Data processing

This Data Processing Agreement and the standard clauses were originally drafted in Dutch. The English version is for convenience only. In case of conflict between the Dutch and the English version, the Dutch version prevails.

Part 1: Data Pro Statement

Along with the Standard Clauses for Data Processing, this Data Pro Statement constitutes the data processing agreement for the product or service provided by the company that has drawn up this Data Pro Statement.

General information

1. **This Data Pro Statement was drawn up by the following Data Processor (verwerker):**
   Boltrics Professionals B.V. (hereinafter also "Boltrics"), Galileïlaan 23b, 6716 BP Ede, The Netherlands, KVK: 08156615, VAT number: NL818818074B01.

   If you have any queries about this Data Pro Statement or data protection in general, please contact:

   For questions regarding this Data Pro Statement, please contact: Mr. Ineke van den Broek, Senior Legal Counsel reachable at legal@boltrics.nl, telephone number: +31 318 742 550.

   For privacy & security questions, please contact: Alexander van den Bosch, Senior Cloud specialist, to be reached at avdbosch@boltrics.nl, telephone number: +31 85 040 32 52.

2. **This Data Pro Statement shall enter into force on [July 2024]**
   We regularly revise the security measures described in this Data Pro Statement to ensure that we are always fully prepared and up to date with regard to data protection. If this document is updated, we shall notify you of the revised versions through our regular channels.

3. **This Data Pro Statement applies to the following products and services provided by data processor**
   Boltrics' software solutions for logistics service providers, consisting of:
   - 3PL Dynamics, with Microsoft Dynamics 365 Business Central underpinning Boltrics' software, which software is modular in nature
   - 3PL Dynamics + Datahub
   - 3PL Dynamics + Web portal v2
   - 3PL Dynamics + Boltrics App Platform

   As well as the support and maintenance services in relation to Boltrics software and other (IT) services provided by Boltrics to its customers as described below and agreed with you.

4. **Description of 3PL Dynamics and services**

   ### 3PL Dynamics

   3PL Dynamics is a Software as a Service (SaaS) application that offers logistics service providers a solution for automating various business processes. Microsoft Business Central lies at the heart of 3PL Dynamics. 3PL Dynamics is modular in structure. The software offers WMS, TMS, Freight Forwarding, Finance, Customs, EDI solution (DataHub) and Customer Portal (Web Portal). For more information about 3PL

Dynamics and its various modules, please refer to the following link: Logistics software: WMS, TMS, FMS, Customs, Finance & CRM | Boltrics.

3PL Dynamics + DataHub

DataHub is an EDI solution that connects to Microsoft Business Central. More information about DataHub can be found under the following link: Easily realize EDI integrations with Boltrics' DataHub | Boltrics.

3PLDynamics + Web Portal

Webportal is a tool that allows customers to unlock data related to inventory management, shipments, quality control, wefts, reports, damages, results and invoices, among others, to their customers. More information about Web Portal can be found under the following link: Customer portal - Boltrics.

3PL Dynamics + Boltrics App Platform

With Boltrics App Platform, customers can extend the capabilities of their logistics software to any mobile device. The App Platform is a single application center for all customer mobile devices. For more information about Boltrics App Platform, please refer to the following link App Platform - Boltrics.

Supporting (IT) services

Besides supplying software, Boltrics offers services such as implementation services, maintenance, support and consultancy work related to its software. For more information on Boltrics' support work, please refer to the following link Support, get your 3PL Dynamics solution back on track | Boltrics.

5. Intended use

General

Our products are designed and equipped to process the following data: All data to perform and support logistics processes in the areas of WMS, TMS, Freight Forwarding, Finance and Customs.

Personal data provided to Boltrics in the context of an order granted to Boltrics for the provision of its services is used exclusively for the performance of the contract entered into by you with Boltrics and other written instructions from you as a data controller, unless a provision of Union or Member State law applicable to Boltrics as a processor requires us to do otherwise. In particular, Boltrics' processing consists of making our applications available with data entered and generated by you available therein. In principle, Boltrics will not add, modify or delete any data without instruction, automated changes may take place during updates if the data structure is thereby technically modified.

Within our software, you can capture various types of personal data. We understand that you may enter all of these, and any personal data or categories you create yourself, and that we will then process them. You are responsible for assessing whether the purpose and nature of the processing is appropriate to our services. You warrant to Boltrics that the processing of personal data as commissioned to Boltrics and/or carried out by you with the help of Boltrics' services, is not in violation of any applicable laws or regulations, is not unlawful and does not infringe any rights of a data subject or third party.

In principle, Boltrics only processes the following personal data for the formation and execution of the agreement or which you register in the context of using the aforementioned services of Boltrics: names,

business contact data such as e-mail addresses and/or telephone numbers and identification data such as login name, password and IP address. Data subjects include representatives and employees of your company and your end users of the Boltrics software including employees and contractors of yours, your customers or suppliers. Before providing personal data to Boltrics, you must obtain all consents from third parties (including contacts, suppliers, contractors and your employees) required under applicable privacy and data protection laws.

3PL Dynamics

3PL Dynamics is designed and set up taking into account the following data considerations: customers manage their own data. Boltrics as processor does not control the data and will only access the data (if possible) at the customer's request or if necessary for the execution of the agreement, e.g. support, and make it available for and at the customer's request. In principle, a limited number of Boltrics employees can access customer data for installation, maintenance and support purposes. They will, unless agreed otherwise or mandatory law requires otherwise, not change or add personal data, but only view it to solve a technical problem.

By using the Microsoft product Business Central underlying 3PL Dynamics or other Microsoft products, personal data are also collected and processed by Microsoft for which Microsoft is responsible since it enters into a contract directly with you for the provision of its services. More information on the intended use and type of personal data processed by Microsoft can be found at Microsoft-privacyverklaring – Microsoft privacy[1] and more specifically in the customer agreement entered into by Microsoft with you: Licensing Documents (microsoft.com).[2]

Only the applications in 3PL Dynamics outside Business Central: DataHub, Web Portal and Boltrics App Platform, are directly managed or hosted by Boltrics.

3PL Dynamics + DataHub

DataHub is designed and set up taking into account the following data considerations: customers manage their own data. Boltrics as processor does not control the data and will only (if possible) access data at the request of the customer or if necessary for the execution of the agreement, e.g. support, and make it available for and at the request of the customer. In principle, a limited number of Boltrics employees can access customer data for installation, maintenance and support purposes. Unless otherwise agreed or mandatory law requires otherwise, they will not change or add personal data, but only view it to solve a technical problem.

3PL Dynamics + Web portal

Web portal was designed and set up taking into account the following data considerations: customers manage their own data. All data from the Business Central environment is stored in the same continental region where the Business Central environment is hosted. Metadata about your company and environment, including the specified company name and logo, as well as pseudonymized data about users, may also be stored in other regions. As a processor, Boltrics does not control the data and will only access data (if possible) at the customer's request or if necessary for the execution of the agreement, e.g. support, and

[1] See Microsoft Privacy Statement - Microsoft privacy for English language. Privacy statement accessed 22-02-2024, subject to and subject to change by Microsoft. Boltrics cannot make any representations, promises or warranties on behalf of Microsoft.
[2] Subject to change by Microsoft.

make it available for and at the customer's request. In principle, a limited number of Boltrics employees can access customer data for installation, maintenance and support purposes. Unless otherwise agreed or mandatory law requires otherwise, they will not change or add personal data, but only view it to solve a technical problem.

3PL Dynamics + Boltrics App Platform

Boltrics App Platform is designed and set up taking into account the following data considerations: customers manage their own data. Boltrics as processor does not control the data and will only (if possible) access data at the request of the customer or if necessary for the execution of the agreement, e.g. support, and make it available for and at the request of the customer. Data is processed anonymously. In principle, a limited number of Boltrics employees can access customer data for installation, maintenance and support purposes. Unless otherwise agreed or mandatory law prescribes otherwise, they will not change or add personal data, but only access it to solve a technical problem. The App Platform stores metadata about your environment in the same continental region as your Business Central environment and possibly in other regions as well.

Support (IT) services.

The following departments within Boltrics process your data for the following activities:

- Administration processes your data for invoicing and contract management. If invoices are not paid even after repeated reminders, Boltrics may engage third parties. In that case, your data, to the extent necessary to collect the claim, will also be provided to these third parties.
- The Purchasing Department communicates with suppliers the contact information you provide to us.
- The Marketing and Sales Department processes your data for personalized information for marketing and sales activities.
- The Consultancy team processes your data to effectively address your issues.
- The Consultancy team processes your data to effectively implement our software solutions with you. This may include, for example, name and contact details of core users and steering committee members.
- The Integration department processes your data to effectively create integrations with your partners. If you provide personal data from these partners, your customers or other suppliers, including IT service providers, to Boltrics, you are responsible for obtaining the express consent of these parties.
- The Support Department processes your personal data to effectively resolve incidents.
- Boltrics IT Ops has full access to customer data for: installing a new version; implementing patches and hotfixes; and managing backups related to the applications that Boltrics manages. With approval from Team Lead IT Ops at Boltrics, employees of the Product Development Department may also be granted temporary access to customer data in necessary cases.

Please provide us with the appropriate contact information for each issue.

When this product/service was designed, the possibility that it would be used to process special categories of personal data or data regarding criminal convictions and offences or personal numbers issued by the government was not taken into account. All products and services were not designed to process special categories of personal data or data regarding criminal convictions and offences or personal numbers issued by the government. It is up to client to determine whether or not it shall use the aforementioned product or service to process such data.

6. **When data processor designed the product or service, it applied a *privacy-by-design/privacy-by-default* approach in the following manner:**
Boltrics uses standard Microsoft designs in its products to apply privacy by design. Microsoft applies privacy by design and privacy by default in its technical and business functions. More information can be found here General Data Protection Regulation - Microsoft GDPR | Microsoft Learn.[3] More on Microsoft Business Central security can be found here Microsoft Business Central security | Learn 3PL Dynamics (boltrics.com). 3PL Dynamics and the underlying Microsoft Business Central database is run on Microsoft Azure. More about Microsoft Azure security can be found here Gegevensbescherming met Microsoft-privacyprincipes | Microsoft Vertrouwenscentrum[4].

For Boltrics' applications (other than Microsoft Business Central) or those managed by Boltrics:
● Applications outside Business Central contain as little data as possible. Whenever possible, data is stored exclusively in Business Central. Personal data is pseudonymized or anonymized whenever possible. Personal data will be stored only in the continental region where the Business Central environment is hosted. Data that allows access to data in Business Central (such as authentication credentials) is stored in a designated additional secure storage in Azure.
● Data stored outside Business Central is viewable from Business Central and can be managed from Business Central by the customer.
Blob data (actual messages), credentials and connection data are stored encrypted in DataHub.
● Data that Boltrics collects for statistical purposes and proactive troubleshooting is processed pseudonymously.
● Personal data is not pseudonymized where/when it is needed for the primary processes (contact with end users).
● Privacy controls are built directly into the system, process or business practice.
● All data in Business Central, App Platform, Web portal and DataHub is encrypted at rest and in transit, in all layers of the architecture and throughout the data lifecycle.
● Boltrics has - unless otherwise agreed/agreed with the customer - by default implemented the most privacy-friendly settings in accordance with its customer's instructions. In addition, where necessary, the respective customer determines which data must be entered or which fields are made available and it is the customer himself who uploads data and enters, deletes and modifies data.

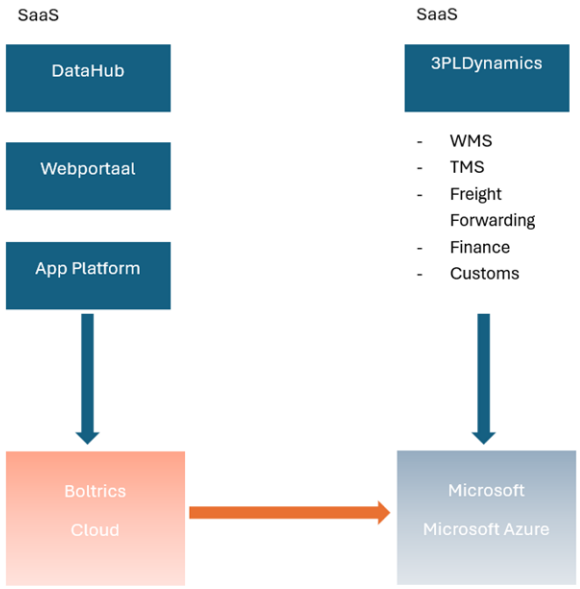
7. **Data processor uses the Data Processing Standard Clauses for data processing, which are attached to the Agreement as an addendum.**

8. **Data Processor processes personal data (partially) outside the EU/EEA. Data processor has ensured in the following way that the personal data shall be protected to an appropriate standard:**
Boltrics processes the personal data of customers within the EU in principle within the EU/EEA and of customers located outside the EU (also) locally where the customer is located. Transfer to countries/sub-processors or processing in countries/by sub-processors outside the EU/EEA may take place if the country in question is subject to an adequacy decision or to sub-processors participating in the EU-US framework, such as Microsoft Corporation, Redmond, WA*[5]. Boltrics will not transfer the personal data to another third country or organization outside the EU/EEA, for which an adequacy decision of the European Commission does not apply, without a written instruction to that effect issued by the customer on legitimate grounds,

[3] General Data Protection Regulation - Microsoft GDPR | Microsoft Learn accessed 22-02-2024, subject to change. Boltrics cannot make any representations, promises or warranties on behalf of Microsoft.
[4] Data Protection with Microsoft Privacy Principles | Microsoft Trust Center, subject to change.
[5] * Based on consultation register Data Privacy Framework as of date 30/01/2024; subject to change, Data Privacy Framework.

binding business rules within the meaning of Article 47, or appropriate safeguards within the meaning of Article 46 AVG. This also includes data storage.

Boltrics uses Cloud outsourcing as shown below:



9. Data processor uses the following sub-processors:

a Microsoft B.V. Evert van de Beekstraat 354, 1118 CZ Schiphol, The Netherlands, Phone: +31 (0)20-500 1500; and

b Microsoft Ireland Operations Limited. Attn: Data Protection Officer, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland. Telephone number: +353 1 706 3117,

For the following Microsoft products in particular: Azure platform, Power Platform (Power BI), Office 365 (Sharepoint, Windows).

Microsoft has major data centers in Australia, Austria, Brazil, Canada, Finland, France, Germany, Hong Kong SAR, India, Ireland, Japan, Korea, Luxembourg, Malaysia, the Netherlands, Singapore, South Africa, the United Kingdom and the United States. The primary storage location is typically in Microsoft's customer region or in the United States, often backed up to a data center in another region.

Microsoft may transfer personal data from the EEA to other countries if there is an adequacy decision by the European Commission or through the use of various legal mechanisms, including contracts such as the standard contractual clauses published by the European Commission under Commission Implementing Decision 2021/914, which ensure an adequate level of protection.[6] The Microsoft privacy statement and more can be found at the following link Microsoft-privacyverklaring – Microsoft privacy.[7]

[6] Microsoft Privacy Statement - Microsoft privacy, dated October 2023, subject to and subject to change. Boltrics cannot make any representations, promises or warranties on behalf of Microsoft.
[7] Microsoft Privacy Statement - Microsoft privacy, subject to change.

In the Microsoft - Boltrics customer relationship, the personal data collected by Microsoft is in principle stored and processed in the Netherlands and Ireland, at least within the EEA, as we are located in the Netherlands as a customer of Microsoft.

For our products we use Microsoft Azure data centers. Since we use Microsoft Azure as a Microsoft customer, Microsoft basically uses the West European data center. For this as well as for the relevant privacy information about Power BI and Office 365 and the local storage of data see Gegevensbescherming met Microsoft-privacyprincipes | Microsoft Vertrouwenscentrum.[8]

10. **Data processor shall support its clients in the following way when they receive requests from data subjects:**
You can create a ticket via support with requests for an export, modification or deletion of data or submit a request to do so via finance@boltrics.nl. If the request involves costs, you will be informed in advance. Boltrics will notify you of any requests received directly from data subjects regarding data subjects' rights under applicable privacy laws, including but not limited to requests for access, rectification, deletion, restriction of processing or transfer of personal data. Boltrics will only comply with such a request if you have instructed Boltrics in writing to do so.

11. **Data Processor shall support its clients with Data Privacy Impact Assessments (DPIA) in the following manner:**
Boltrics will cooperate with Data Privacy Impact Assessments in the following manner:
- You will contact Boltrics by email at finance@boltrics.nl
- You make clear what assistance you require from Boltrics
- Boltrics will provide the desired cooperation as soon as possible and may charge additional costs in accordance with its usual hourly rate.

12. **After termination of the Agreement concluded with you, Boltrics will in principle delete the personal data it processes for you within 3 months in such a way that it can no longer be used and is no longer accessible (render inaccessible)**, unless the data is necessary for marketing purposes or Boltrics is required to observe a different period by virtue of the agreement concluded with you, this Processing Agreement, or the law. If, in your judgment and as the person responsible for the personal data, certain personal data should or need not be kept longer and the law does not provide otherwise, Boltrics will, upon your written request, destroy the specified personal data and certify to you that it has done so.

Security policy

13. Data processor has implemented the following security measures to protect its product or service:
Boltrics has taken security measures to protect its product or service and treats your data with the utmost care. We process your data only in accordance with the requirements of applicable privacy legislation. This means that:
- *We secure your personal data at an adequate and appropriate level.*
- *We do not share your personal data in any way with third parties unless: I) we have obtained prior consent from you as detailed in the Processing Agreement and have established a processing agreement with the third party we are working with, or II) we are required by law to provide your data, for example for investigation by government agencies such as judicial or regulatory authorities.*

[8] Data Protection with Microsoft Privacy Principles | Microsoft Trust Center, subject to change.

- *We do not retain your personal data for longer than necessary to fulfil the purposes for which your data was provided or collected.*
- *Part of security is confidentiality. Everyone working with personal data within Boltrics has a duty of confidentiality. This confidentiality is guaranteed within Boltrics by signing a confidentiality declaration or a confidentiality clause in the employment contract.*
- *The confidentiality, integrity, availability and resilience of the product or service is primarily guaranteed by the fact that Microsoft products underpin Boltrics' product or service. Business Central or Microsoft Azure, underlying Boltrics' software, as far as the Microsoft SaaS environment is concerned, comply with the following standards and certifications of Microsoft*, among others:*

  1. *ISO 9001:2015*
  2. *SOC 1 (SSAE 18) Type 2.*
  3. *SSAE 16 / ISAE 3402*
  4. *ISO 27001*
  5. *ISO/IEC 20000-1:2011*
  6. *ISO/IEC 27018.*[9]

- *There is in principle a strict (with at least logical) separation of data per client.*
- *Personal data is stored encrypted.*
- *Restoring or granting access to data or information, of whatever nature, will only take place after an order from the client if it cannot be established exclusively that this data or information belongs to an authorized person (from the client's organization) or that this person should have access to it.*
- *Use of anti-virus, anti-malware short of security software is forced.*
- *Complex passwords in combination with multi-factor authentication are used in the (internal) management of systems.*
- *Within Boltrics there is centralization and uniformity of access to customer environments and insight into who/when has access.*
- *Boltrics employees work according to a code of conduct. This includes agreements on security and privacy.*
- *Boltrics Employees are obliged to attend security awareness trainings.*
- *Laptops/computers are managed via Microsoft Intune, with Boltrics using virus scanners/antimalware and Windows updates to ensure all systems are up-to-date and secure.*
- *In Boltrics' Azure environment, Boltrics has ensured that production servers are separated from test and development servers through separate virtual networks. This minimizes Boltrics' risk of unauthorized access and keeps Boltrics' (confidential) data safe. DataHub, Core and API run in a*

[9] *summary included on [30/01/2024] and is subject to change; does not constitute a warranty, including on behalf of Microsoft, Boltrics cannot make any commitments or undertakings on Microsoft's behalf. Microsoft manages Microsoft Cloud (Azure) or its environments and is responsible for its products. For Microsoft certifications, Boltrics refers to the following link Compliance offerings for Microsoft 365, Azure, and other Microsoft services. | Microsoft Learn. More about Microsoft Business Central security can also be found under the following link: Microsoft Business Central security | Learn 3PL Dynamics (boltrics.com).

separate virtual network, accessible only from the virtual network or POST functionality. POST runs outside virtual network, access is restricted with basicAuth and/or API Key and/or whitelisting.

- *Boltrics' Azure server security is through Microsoft Defender for Cloud, which allows Boltrics to actively detect threats and respond quickly to maintain the integrity of its systems.*
- *Multi-Factor Authentication is required for employees: to access the network remotely; to protect admin (privileged) accounts; and to access all cloud resources, including Office365.*
- *Implementation of SPF, DKIM and DMARC to protect against forged emails.*
- *Regular full and additional (incremental) backup of corporate data is performed; Backups are tested for recoverability; Backups are created in Azure Geo Redundant Storage.*
- *Boltrics implements full disk encryption on all its laptops and workstations that may access, process and/or store sensitive information. Boltrics uses additional cryptographic mechanisms to encrypt sensitive customer data generated/exchanged for support purposes, credentials allowing access to customer resources are stored in an encrypted Azure Key Vault.*
- *The system/service provided by Boltrics uses technical control(s) to encrypt sensitive information during transit.*
- *Data classification in the application on Business Central further ensures that most requests from data subjects regarding access, deletion, modification or data portability of personal data can be met quickly and that in the event of an incident, in many cases the availability of and access to the personal data can be restored in a timely manner.*
- *There is a procedure on dealing with and handling data breaches.*

14. **Data processor conforms to the principles of the following Information Security Management System (ISMS):**
Boltrics strives to conform to the Information Security Management System (ISMS) Microsoft Security Development Lifecycle and Cyber essentials standard. At Boltrics, we are continuously working on conforming to (new) standards. As soon as necessary, we will update the processing agreement accordingly.

15. **Data processor has obtained the following certificates**
- Data Pro Certificate (*After positive completion of registration process*).
- Boltrics has obtained the Certified for Microsoft Dynamics seal of approval, the highest standard for partner-developed software.

Data leak protocol

16. **In the unfortunate event something does go wrong, data processor shall follow the following data breach protocol to ensure that clients are notified of incidents:**
If Boltrics discovers a potential data breach, Boltrics will inform you, the customer, without undue delay, in accordance with the obligations set forth in the Data processing agreement.

Boltrics will, if possible, provide you with information on at least the following: (i) the nature of the breach, where possible specifying the categories of data subjects affected and, approximately, the number of data subjects affected; (ii) the personal data (potentially) affected and, approximately, the number of personal data affected; (iii) the identified and expected consequences of the breach for the processing of the personal data and the persons affected thereby; and (iv) the measures that Boltrics has taken and will take to address the breach, including, where applicable, the measures to mitigate any negative consequences of the breach.

The notification will be addressed by Boltrics to a contact person to be designated by you. You must provide Boltrics with written contact information for this contact person. The notice will be given either by telephone or by e-mail. Upon receipt of the notification, you will inform Boltrics of how you will, if necessary, report any data breach to the Personal Data Authority.

Whether or not to report remains the responsibility of you as the data controller (Article 33 GDPR). Upon request, Boltrics will support you in the reporting process.

Boltrics will take reasonable measures necessary to limit the (possible) damage of a security breach.

Part 2: Standard Clauses for Data Processing

Version: November 2019

Along with the Data Pro Statement, these standard clauses constitute the data processing agreement. They also constitute an annex to the Agreement and to the appendices to this Agreement, e.g. any general terms and conditions which may apply.

Article 1. Definitions

The following terms have the following meanings ascribed to them in the present Standard Clauses for Data Processing, in the Data Pro Statement and in the Agreement:

1.1 **Dutch Data Protection Authority (AP):** the supervisory authority defined in Section 4.21 of the GDPR.

1.2 **GDPR:** the General Data Protection Regulation.

1.3 **Data Processor**: the party which, in its capacity as an ICT supplier, processes Personal Data on behalf of its Client as part of the performance of the Agreement.

1.4 **Data Pro Statement**: a statement issued by the Data Processor in which it provides information such as the intended use of its products and/or services, any security measures which have been implemented, sub-processors, data breach, certification and dealing with the rights of Data Subjects.

1.5 **Data Subject**: a natural person who can be identified, directly or indirectly.

1.6 **Client:** the party on whose behalf Data Processor processes Personal Data. Client can either be the controller (the party who determines the purpose and means of the processing) or another data processor.

1.7 **Agreement**: the agreement concluded between Client and Data Processor, based on which the ICT supplier provides services and/or products to Client, the data processing agreement forming part of this agreement.

1.8 **Personal Data** any and all information regarding a natural person who has been or can be identified, as defined in Article 4.1 of the GDPR, processed by Data Processor to meet its requirements under the Agreement.

1.9 **Data Processing Agreement**: the present Standard Clauses for Data Processing , which, together with Data Processor's Data Pro Statement (or similar such information), constitute the data processing agreement within the meaning of Article 28.3 of the GDPR.

Article 2. General provisions

2.1 The present Standard Clauses for Data Processing apply to all Personal Data processing operations carried out by Data Processor in providing its products and services, as well as to all Agreements and offers. The applicability of Client's data processing agreements is explicitly rejected.

2.2 The Data Pro Statement, and particularly the security measures described in it, may be adapted from time to time to changing circumstances by Data Processor. Data Processor shall notify Client in the event of significant revisions. If Client in all reasonableness cannot agree to the revisions, Client shall be entitled to terminate the data processing agreement in writing, stating its reasons for doing so, within thirty days of having been served notice of the revisions.

2.3 Data Processor shall process the Personal Data on behalf of Client, in accordance with the written instructions provided by Client and accepted by Data Processor.

2.4 Client or its customer shall serve as the controller within the meaning of the GDPR, shall have control over the processing of the Personal Data and shall determine the purpose and means of processing the Personal Data.

2.5 Data Processor shall serve as the processor within the meaning of the GDPR and shall therefore not determine the purpose and means of processing the Personal Data, and shall not make any decisions on the use of the Personal Data and other such matters.

2.6 Data Processor shall implement the GDPR as laid down in the present Standard Clauses for Data Processing, the Data Pro Statement and the Agreement. It is up to Client to assess, on the basis of this information, whether Data Processor is providing sufficient guarantees with regard to the implementation of appropriate technical and organisational measures in order to ensure that the processing operations meet the requirements of the GDPR and that Data Subjects' rights are sufficiently protected.

2.7 Client shall guarantee Data Processor that it acts in accordance with the GDPR, that it provides a high level of protection for its systems and infrastructure at all time, that the nature, use and/or processing of the Personal Data are not unlawful and that they do not violate any third party's rights.

2.8 Administrative fines imposed on Client by the Dutch Data Protection Authority cannot be recovered from Data Processor.

Article 3. Security

3.1 Data Processor shall implement the technical and organisational security measures set out in its Data Pro Statement. In implementing the technical and organisational security measures, Data Processor shall take into account the state of the art and the costs of implementation, as well as the nature, scope, context and purposes of the processing and the intended use of its products and services, and the risk in processing the data of varying likelihood and severity inherent to the rights and freedoms of Data Subjects that are to be expected considering the nature of the intended use of Data Processor's products and services.

3.2 Unless explicitly stated otherwise in the Data Pro Statement, the products and services provided by Data Processor shall not be equipped to process special categories of personal data or data relating to criminal convictions and offences.

3.3 Data Processor seeks to ensure that the security measures it shall implement are appropriate for the manner in which Data Processor intends to use the products and services.

3.4 In Client's opinion, said security measures provide a level of security that is tailored to the risk inherent in the processing of the Personal Data used or provided by Client, taking into account the factors referred to in Article 3.1.

3.5 Data Processor shall be entitled to adjust the security measures it has implemented if to its discretion such is necessary for a continued provision of an appropriate level of security. Data Processor shall record any significant adjustments it chooses to make, e.g. in a revised Data Pro Statement, and shall notify Client of said adjustments where relevant.

3.6 Client may request Data Processor to implement further security measures. Data Processor shall not be obliged to honour such requests to adjust its security measures. If Data Processor makes any adjustments to its security measures at Client's request, Data Processor is entitled to invoice Client for the costs associated with said adjustments. Data Processor shall not be required to actually implement the requested security measures until both Parties have agreed upon them in writing. .

Article 4. Data breaches

4.1 Data Processor does not guarantee that its security measures shall be effective under all circumstances. If Data Processor discovers a data breach within the meaning of Article 4 sub 12 of the GDPR, it shall notify Client without undue delay. The "Data Breach Protocol" section of the Data Pro Statement outlines the way in which Data Processor shall notify Client of data breaches.

4.2 It is up to the Controller (the Client or its customer) to assess whether the data breach of which Data Processor has notified the Controller must be reported to the Dutch Data Protection Authority or to the Data Subject concerned. The Controller (Client or its customer) shall at all times remain responsible for reporting data breaches which must be reported to the Dutch Data Protection Authority and/or Data Subjects pursuant to Articles 33 and 34 of the GDPR. Data Processor is not obliged to report data breaches to the Dutch Data Protection Authority and/or to the Data Subject.

4.3 Where necessary, Data Processor shall provide further information on the data breach and shall assist Client to meet its breach notification requirements within the meaning of Articles 33 and 34 of the GDPR by providing all the necessary information available to Data Processor.

4.4 If Data Processor incurs any reasonable costs in doing so, it is entitled invoice Client for these, at the rates applicable at the time.

Article 5. Confidentiality

5.1 Data Processor shall ensure that the persons processing Personal Data acting under its authority have committed themselves to confidentiality.

5.2 Data Processor shall be entitled to provide third parties with Personal Data if and insofar as such is necessary due to a court order, statutory provision or order issued by a competent government authority.

5.3 Any and all access and/or identification codes, certificates, information regarding access and/or password policies provided by Data Processor to Client, and any and all information provided by Data Processor to Client detailing the technical and organisational security measures included in the Data Pro Statement are

confidential and shall be treated as such by Client and shall only be disclosed to authorised employees of Client. Client shall ensure that its employees comply with the requirements described in this article.

Article 6. Term and termination

6.1 This data processing agreement constitutes part of the Agreement, and any new or subsequent agreement arising from it and shall enter into force at the time of the conclusion of the Agreement and shall remain effective for an indefinite period.

6.2 This data processing agreement shall end by operation of law upon termination of the Agreement or upon termination of any new or subsequent agreement arising from it between parties.

6.3 If the data processing agreement is terminated, Data Processor shall delete all Personal Data it currently stores and which it has obtained from Client within the timeframe laid down in the Data Pro Statement, in such a way that the Personal Data can no longer be used and shall have been *rendered inaccessible*. Alternatively, if such has been agreed, Data Processor shall return the Personal Data to Client in a machine-readable format.

6.4 If Data Processor incurs any costs associated with the provisions of Article 6.3, it shall be entitled to invoice Client for said costs. Further arrangements relating to this subject can be laid down in the Data Pro Statement.

6.5 The provisions of Article 6.3 do not apply if Data Processor is prevented from removing or returning the Personal Data in full or in part by a statutory provision. In such instances, Data Processor shall only continue to process the Personal Data insofar as such is necessary by virtue of its statutory obligations. Furthermore, the provisions of Article 6.3 shall not apply if Data Processor is the Controller of the Personal Data within the meaning of the GDPR.

Article 7. The rights of Data Subjects, Data Protection Impact Assessments (DPIA) and auditing rights

7.1 Where possible, Data Processor shall cooperate with reasonable requests made by Client relating to Data Subjects who invoke their rights from Client. If Data Processor is directly approached by a Data Subject, it shall refer the Data Subject to Client where possible.

7.2 If Client is required to carry out a Data Protection Impact Assessment or a subsequent consultation within the meaning of Articles 35 and 36 of the GDPR, Data Processor shall cooperate with such, following a reasonable request to do so.

7.3 Data Processor shall be able to demonstrate its compliance with its requirements under the data processing agreement by means of a valid Data Processing Certificate or an equivalent certificate or audit report (third-party memorandum) issued by an independent expert.

7.4 In addition, at Client's request, Data Processor shall provide all other information that is reasonably required to demonstrate compliance with the arrangements made in this data processing agreement. If, in spite of the foregoing, Client has grounds to believe that the Personal Data are not processed in accordance with the data processing agreement, Client shall be entitled to have an audit performed (at its own expense) not more

than once every year by an independent, certified, external expert who has demonstrable experience with the type of data processing operations carried out under the Agreement. The scope of the audit shall be limited to verifying that Data Processor is complying with the arrangements made regarding the processing of the Personal Data as set forth in the present data processing agreement. The expert shall be subject to a duty of confidentiality with regard to his/her findings and shall only notify Client of matters which cause Data Processor to fail to comply with its obligations under the data processing agreement. The expert shall furnish Data Processor with a copy of his/her report. Data Processor shall be entitled to reject an audit or instruction issued by the expert if to its discretion the audit or instruction is inconsistent with the GDPR or any other law, or that it constitutes an unacceptable breach of the security measures it has implemented.

7.5 The parties shall consult each other on the findings of the report at their earliest convenience. The parties shall implement the measures for improvement suggested in the report insofar as they can be reasonably expected to do so. Data Processor shall implement the proposed measures for improvement insofar as to its discretion such are appropriate, taking into account the processing risks associated with its product or service, the state of the art, the costs of implementation, the market in which it operates, and the intended use of the product or service.

7.6 Data Processor shall be entitled to invoice Client for any costs it incurs in implementing the measures referred to in this article.

Article 8. Sub-processors

8.1 Data Processor has specified in the Data Pro Statement whether Data Processor uses any third parties (subprocessors) to help it process the Personal Data, and if so, which third parties.

8.2 Client hereby authorises Data Processor to hire other sub-processors to meet its obligations under the Agreement.

8.3 Data Processor shall notify Client of any changes concerning the addition or replacement of the third parties (sub-processors) hired by Data Processor, e.g. through a revised Data Pro Statement. Client shall be entitled to object to such changes . Data Processor shall ensure that any third parties it hires shall commit to ensuring the same level of Personal Data protection as the security level Data Processor is bound to provide to the Client pursuant to the Data Pro Statement.

Article 9. Other provisions

These Standard Clauses for Data Processing, along with the Data Pro Statement, constitute an integral part of the Agreement. Therefore, any and all rights and obligations arising from the Agreement, including any applicable general terms and conditions and/or limitations of liability, shall also apply to the data processing agreement.

Do you have questions?

Our legal experts can foresee you in advice and help. Please do contact us.

NLdigital organises various legal workshops and gatherings. Keep an eye on the calendar on our website. Members of NLdigital can participate in this workshops and gatherings for free. When you're not a member and you want to take advantage of this and many other possibilities that our membership has to offer? Check out the advantages.

NLdigital BV
De Corridor 5
3621 ZA Breukelen

juristen@nldigital.nl
+31 (0) 348 - 49 36 36

KVK 71675574

NLdigital